COMPUTER SYSTEM SECURITY AND PRIVACY ADVISORY BOARD SUMMARY OF MEETING

National Institute of Standards and Technology Gaithersburg, MD June 13-15, 2000

Tuesday, June 13, 2000

Board Chairman, Mr. Franklin S. Reeder, convened the Computer System Security and Privacy Advisory Board for its second meeting of the year at 9:00 A.M.

Board members present in addition to the Chairman were:

Mr. Peter Brown
Mr. Richard Guida
Mr. Daniel Knauf
Mr. Joseph Leo
Mr. Stephen Lipner [in attendance June 14-15 only]
Mr. John Sabo [in attendance June 14-15 only]
Mr. James Wade
Mr. Rick Weingarten
Ms. Karen Worstell

Also attending was member designate Ms. Michelle Moldenhauer. She will be filling a federal government representative vacancy.

Mr. Ed Roback, Board Secretary reviewed the agenda and the handout materials for the 3-day meeting. The first two days of this meeting were dedicated to a workshop on approaches to security metrics. A 'white paper' summary of that portion of the meeting is attached to these minutes. Mr. Roback discussed the current membership status of the Board and noted that there was one federal government vacancy at this time. He also announced that Mr. Franklin Reeder was recently appointed by the Director of NIST to serve as the new Chairman of the Board.

The entire meeting was open to the public. There were 30 people from the public in attendance when the meeting was called to order.

Opening Remarks by Chairman

Franklin S. Reeder

Mr. Reeder expressed his delight at being part of the Board and the honor in following past Chairman Willis Ware. He encouraged the input from the membership on potential candidates to fill future Board vacancies. He also asked them to think about how the Board could be a constructive force in accomplishing its mandate.

The Chairman introduced Dr. Fran Nielsen, workshop coordinator, who covered the focus issues of the workshop. This was followed by the various workshop presentations and discussion. A summary of this workshop activity is attached. All available presentation materials from this workshop are listed on the following website: www.csrc.nist.gov/csspab/.

The workshop/meeting was recessed for the day at 4:45 p.m.

Wednesday, June 14, 2000

Chairman Reeder reconvened the meeting at 9:00 a.m. Dr. Nielsen presented a summary of day one of the workshop and continued with the presentations for the day.

The workshop/meeting was recessed for the day at 4:40 p.m.

Thursday, June 15, 2000

Chairman Reeder reconvened the meeting at 9:10 a.m.

Discussion of Potential Follow-On Activities

On reflection of the previous two-day workshop, Mr. Reeder said that the objectives were to bring together a group of well-informed theorist and practitioners to give the Board a sense of what was going on in the metrics area. He expressed the Board's gratitude to Dr. Nielsen and Mr. Roback for putting together a great program.

Next, Mr. Reeder addressed the Board developing a set of next steps to be taken on computer security and privacy issues, such as security metrics. Given the Board's charter, scope and limitations, they should examine where they can be of value. He said that he is impressed with the quality of those who sit on the Board and wants to see that continue. Given these qualities and capabilities and the nature of the world today, how can this group make a difference, Reeder stated.

With regard to security metrics and what the Board heard over the past two days, Mr. Reeder asked to what extent the work of the federal government, as lead by the CIO council, is consistent with what the Board heard about the development of metrics.

Board Member Guida's observation was that the CIO Council is very much in the process of feeling out what the role should be. There has been more activity within the last year. Under the Committee structure, the CIO is producing some output. He said that they have adopted more of a focus on trying to get out something useful.

Board Member Knauf said that he is seeing a more informal movement to increase coordination and cooperation between the CIO Council and other existing groups. He cited a recently issued formal memorandum from the CIO Council on the subject of certification and validation processes that could be applied to the NSTISSC community.

Board Member Leo shared some of his thoughts on how the Board can be of greater value. The Board should keep in mind that this is an election year and that interface with the transition team is essential to how we may want to posture ourselves as a Board. The Board should also keep abreast of the legislation that is moving on the Hill that may pertain to them. However, he feels that it is important that we be realistic about where the Board can go, given the lack of funding. Leadership in OMB continues to search for its role to the federal agencies in regards to stewardship. He believes that the CIO Council, and its Security Committee in particular, would welcome more active, pragmatic participation from the Board. Also, there is a need for more interaction and representation by the civilian agencies. His point of view is that the Board needs to step back from its "inquiry and listening" mode and become more active.

Chairman Reeder expressed the need for more active participation by the civilian agencies in some of the DOD world program activities in order to add a civil agency face on that work. The civil agencies could have an opportunity to gain some leverage here. There should also be a strong emphasis and obligation applied on the DOD world to make certain that where it produces products, that it consider the utility of those products for the civilian sector.

One of the biggest issues that face all of the arenas is taxonomy, stated Board Member Knauf, and he proposed that the Board take a look at this issue. He said that this is another strong reason for the conjoining/cooperation between civilian and national security. He stated the problem as when you get away from security as the operating work and begin to look at assurance, etc, there is less distinctiveness then there was before. Interdependence and dimensions of the taxonomies cause blurring.

Board Member Guida mentioned that there was very strong harmonization between the DOD and civilian agencies in the PKI work arenas. Both are working together and exchanging information, therefore, getting first hand input.

Ed Roback said that NIST has been working to capitalize on existing things as opposed to reinventing them. Recently, NIST reviewed a NSTISSC directive and added to it what was applicable to the civilian sector. NIST also worked with the CIO Council on the draft security framework model document. It will be distributed for comment shortly and implementation guidance will follow.

Chairman Reeder asked how the Board could advance the work of the CIO Council's security framework document.

Board Member Browne said that the Board has learned that the model that has been produced is just one aspect and that this Board can and should influence that in a major way. The Board should help them unify it or make that model whole.

Board Member Sabo said that the Board is in a position to conduct workshops, to produce documents, etc., and that we should recognize that we are not going to do the work of the CIO Council. However, we should provide very direct input and guidance to them. It is also his view that the value of the Board is the membership and its ability to set an agenda, set a strategy and the luxury of building a small program around it.

Michelle Moldenhauer said that she sees the Board as an advisory committee. She likes the idea of having industry as part of the effort. The CIO Council does not have that. She also pointed out that the Board's mandate calls for them to also advise OMB.

How CSSPAB Can Make a Difference

Chairman Reeder presented a brief overview to stimulate dialogue among the members. He covered the drivers and constraints of the Board. He reviewed the statements in the Computer Security Act of 1987 pertaining to the duties and obligations of the Board. He said that the Act gives the Board an incredibly broad mission with access to just about everyone. It has an obligation to report its findings. Major constraints, however, are the Federal Advisory Committee Act requirements and the budget. Objectives include knowledge transfer between private sector to government and military sector to civil sector; identifying and weighing in on issues, advancing the 'state of the practice,' etc. The Board can select an issue and take a specific position on it. Potential areas of interest/focus include metrics and report cards; resources for security and privacy, staff competence; organization for security and privacy in the Executive Branch and in the Congress and NIST programs.

Suggested means and methods to accomplish these objectives include how often meetings should be held and where should they be held, workshops, conferences, sponsored "research",

technology via web sites and list servers. Advocacy is an effort that can be undertaken by the non-Federal members of the Board.

Chairman Reeder encouraged the members of the Board to dialogue with some of the stakeholders about the efforts of the Board and what they see could be done. He has already met with representatives from the General Services Administration, National Security Council, NIST and OMB.

Ray Kammer, Director of NIST, was invited to address the Board on its role. He pointed out that the current problems are not where the Board should be setting their agenda but rather three or four months out. First of all, he believes that the Board is a good pulpit to speak from. Secondly, Congress has a lot of naivete on computer security related issues as evidenced by the recent attacks on the websites.

Another realm is how the government organizes itself. There is a clear distinction between the classified and non-classified world. He noted that over the last several years, the government has made the decision to invest resources in the Department of Justice in the area of computer security and privacy. He also pointed out that the Board does have a uniqueness that does not exist in other Boards.

On the topic of budget for NIST in the computer security area, he said that there had been a request in the last budget proposal for an additional amount of money for computer security. The House did not approve this increase. However, Mr. Kammer did feel somewhat encouraged that the Senate would reinstate $5M for research and development in computer security. The picture does look grim for funding for assistance to other agencies because the Congress feels that agencies can figure out their own problems.

In response to Joe Leo's question about the NIST computer security program, Mr. Kammer said that he had pushed hard in the budget process to get money for computer security. He cited the recent computer security efforts of the President's Committee of Advisors on Science and Technology (PCAST) as one example of the Administration's major focus on computer security needs. With regard to the lack of a senior level position to head the NIST computer security division, Mr. Kammer said that the Department of Commerce is not approving any SES positions in any of its agencies, regardless of what the program is.

Board Member Sabo suggested that the NIST Computer Security Division could use the staff support of one more person to help assist the Board effort.

Board Member Knauf recommended that the Board consider communicating to Congressional committee leaders and the Speaker of the House on the structure of Congressional committees with regard to better oversight. Mr. Kammer said that certainly better oversight would be beneficial but would be difficult to achieve. He does, however, believe that it would be a good thing for the Board to go on record with their suggestions, but not have any expectation of any future success in this area.

Bill Mehuron, Information Technology Division Laboratory Director, stated that the Lab has a strong commitment to the NIST computer security program and that their budget has increased as well as the staffing.

Glenn Schlarman, Office of Information and Regulatory Affairs, OMB, was next to address the Board. He began his remarks by saying that it was one of his goals to have people say "what does CSSPAB think…." He feels that CSSPAB should be an organization whose opinion is valued outside of its meeting room. OMB needs an organization that gets the briefings, gathers the information and then synthesizes it. It needs output. It needs to know what the Board thinks is important. He said that the Board should also look at the privacy issues. He believes that the Board has a unique perspective to bring because of its make up of representatives. The topic

de jour is the Federal CIO or Federal CISO. If the Board believes it is important, they should take it on and offer their opinions.

Chairman Reeder believes that the Board should decide where OMB should more formally weigh in on specific topics rather than have OMB formally solicit the Board for advice. Mr. Schlarman stated that OMB would not tell the group what they should be doing.

Board Member Leo urged OMB to continue to raise the importance of computer security within NIST. He believes that NIST is the foundation and pillar of computer security within the federal government. He also feels that if there is to be a computer security czar that they should be placed within NIST and that it should be a rotational-type position.

Ways to address pervasive computer security and privacy issues has also been a challenge for the private sector, reported Board Member Worstell. She believes that the Board needs to be a lightening rod to identifying issues that are worth weighing in on. She also suggested that the Board work from the high end down stating that there is difficulty in pushing things up to the top from the lower end where they have identified major issues. There should be identification of long-range computer security and privacy issues that will show the risk 12-18 months out.

In closing, Mr. Schlarman stated that security is an essential element but not the only essential element. It is a fundamental issue that has to be addressed, however. When it impedes the mission, it will be ignored, worked around, etc. The challenge is to come up with a built-in security framework.

Chairman Reeder had also invited John Tritak of the CIAO, Tom Burke of GSA and Jeffery Hunker of NSC to present their views but they were unable to attend because of schedule conflicts.

Next, Board Member Worstell presented the members with a copy of a draft of ideas and focus starting points for the Board to consider [ref. #1]. It proposes the establishment of a cross agency governance, establishment of a approach of baseline controls, possible adoption of a national standard for information security management, and establishment of a federal/private sector best practice sharing The members were asked to provide their comments within 10 days and she would recirculate it to the members for their information.

Half of the CIO Council members will be gone as a result of the election as they hold political appointee positions, noted Board Member Leo. He estimates that it will be over nine months before any new CIOs are in place to participate on the Council. He suggested that an entity be established in the area of cross agency governance regardless of the activities of the CIO Council.

Chairman Reeder recapped several of the suggestions the Board had made in their discussions.

(1) Produce substantive advice on how the government deals with information assurance. Development of a common taxonomy (of terms) is needed. This is particularly urgent given the upcoming transition in the Administration.

(2) Assess and advise the CIO Council on their proposed metrics framework document.

(3) Help the government/NIST to define its security and privacy agenda by identifying the issues over the horizon.

(4) What are the implications of a 24/7 government, i.e. GPEA, E-Commerce, etc. Does everyone really understand the risks. The Board could form the policy debate around this issue, i.e., there are more than technical problems that may be encountered.

(5) What should a baseline look like? Does a baseline approach make sense? There is a need for a minimum standards and acceptability approach.

(6) Identify resource areas for computer security efforts; be an advocate when necessary.

(7) Important to have a working actions list. Identify the general focus with flexibility to shift to other areas from time to time. Need to see more reporting of positions, issues, findings, etc.

(8) Focus on privacy issues and e-commerce. Raise awareness by conducting public workshops/conferences perhaps similar to the security metrics workshop.

(9) Need for development of Board opinions on legislation such as S.1993 and HR 2413, the CIAO national plan and other current issues. Suggested formation of a working group to review the national plan to report back to the Board with suggested positions/issues.

Discussion of this list will continue at the next meeting.

Other actions/observations included:

(1) Review of Karen Worstell's proposal and provide comments to her prior to the next meeting.

(2) Development of overall agenda paper by Chairman Reeder.

(3) Development of a white paper by Fran Nielsen as a result of the security metrics workshop. This will be a discussion topic at the September meeting.

(4) Comments on the CIO maturity model document will be provided to Steve Lipner and John Sabo for coordination of a Board position.

(5) Discussion of the mechanisms that the Board may want to take to accomplish some of the identified goals. Identify one subject area where the Board could host a workshop; yearly plan one larger public event.

(6) Recent metrics workshop was just a kick-off of an important topic. Need to be sure to continue with this topic.

(7) Legislative maters often don't allow the Board appropriate time to be reactive. Need to develop a way to address these matters in a timely manner.

(8) Establish an open forum on the web where members can identify issues that need to be looked at as well as solicit input from other interested parties.

(9) Dan Knauf will share with the Board a list of 'hot' topics that he has developed.

There be no further business, the Chairman adjourned the meeting at 12:50 p.m.

Attachment – Security Metrics Workshop White Paper

Reference #1 – Worstell draft of focus points

Edward Roback
Board Secretary

CERTIFIED as a true and accurate
summary of the meeting.

Franklin S. Reeder
Chairman

.